Revealing Side-Channel Issues of Complex Circuits by Enhanced Leakage Models

Annelie Heuser*†, Werner Schindler†‡, and Marc Stöttinger*†
*ISS - Integrated Circuit and Systems Lab, Technische Universität Darmstadt,
64289 Darmstadt, Germany
Email: {heuser,stoettinger}@iss.tu-darmstadt.de
†CASED - Center for Advanced Security Research Darmstadt,
64293 Darmstadt, Germany
‡BSI - Bundesamt für Sicherheit in der Informationstechnik
53175 Bonn, Germany
Email: werner.schindler@bsi.bund.de

***Abstract*—In the light of implementation attacks a better understanding of complex circuits of security sensitive applications is an important issue. Appropriate evaluation tools and metrics are required to understand the origin of implementation flaws within the design process. The selected leakage model has significant influence on the reliability of evaluation results concerning the side-channel resistance of a cryptographic implementation. In this contribution we introduce methods, which determine the accuracy of the leakage characterization and allow to quantify the signal-to-noise ratio. This allows a quantitative assessment of the side-channel resistance of an implementation without launching an attack. We validate the conclusions drawn from our new methods by real attacks and obtain similar results. Compared to the commonly used Hamming Distance model in our experiments enhanced leakage models increased the attack efficiency by up to 500%.**

Key words: signal-to-noise ratio, approximation error, constructive side-channel analysis, secure hardware design

I. Introduction

Since the mid-nineties side-channel attacks have constituted serious threats to security implementations. Usually, either profiling-free attacks (like *simple power analysis (spa)* [1], *differential power analysis (dpa)* [1], *correlation power analysis (cpa) [2]*, or *mutual information analysis (mia) [3]*) or profiling-based methods (like *Template Attacks* [4] or the *stochastic approach* [5]) are used to check the vulnerability of cryptographic implementations by side-channel attacks. Many side-channel attacks apply simple leakage models to exploit the power consumption, assuming bitwise independent side-channel leakage (e.g., the Hamming Distance or the Hamming Weight for single-bit or multi-bit leakage models). However, [6]–[8] clearly point out that complex leakage models (in combination with linear regression analysis) are often more effective than the commonly used simple leakage models since they map the switching activity of the circuit more precisely to estimated power consumption. Linear regression analysis allows to reduce the number of parameters, which have to be considered. But how can a designer decide whether the considered leakage characterization is precise enough, and which model is most efficient for a given implementation?

In this article we develop two methods, which help to answer these questions. The first method considers the accuracy of the selected leakage function, which quantifies the leakage model. More precisely, it provides an estimate for the approximation error of the (estimated) leakage function, which has been derived on basis of the selected leakage model. The second method quantifies the signal-to-noise ratio for arbitrary leakage models. We demonstrate both the application and the benefit of the introduced new methods (viewed as design-supporting tools) for several leakage models. The proposed methods are based on the *stochastic approach*, which was originally designed as an attack instrument to disclose a secret cryptographic key of a block cipher [5], [9]–[12]. We explain how the first profiling step of the stochastic approach can be used by hardware designers in order to obtain information of the selected leakage function accuracy and of the acquisition quality. These information can constructively be used to design effective countermeasures and to gain insights in security-critical properties of an implementation.

In Sect. II we briefly sketch the basics of the stochastic approach. In Sect. III we discuss several leakage models and explain which internal effects of the circuit they should capture. A method to estimate the approximation error of the leakage function is developed in Sect. IV, which allows the designer to quantify the accuracy of the leakage function. In Sect. V we show how the stochastic approach can be used to estimate the signal-to-noise ratio, which in turn determines the quality of the measurable leakage of a circuit. Besides theoretical reasoning a case study (including attacks) for a hardware implementation of the *Advanced Encryption Standard (AES)* [13] is conducted. Section VI concludes the contribution.

978-3-9810801-8-6/DATE12/© 2012 EDAA

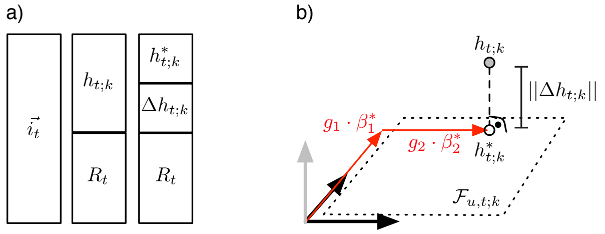

Fig. 1. a) Relation between the stochastic model and the current consumption b) Subspace representation of the data-dependent current consumption

II. Constructive Side-channel Analysis

The general idea of constructive side-channel analysis is to gain quantitative information on the side-channel leakage and to use it for the (re-)design. In [8] it was demonstrated how the first profiling step of the stochastic approach can be used to quantify the data-dependent power consumption and thus to support (re-)design constructively. Moreover, in [14] a new symmetry metric was introduced to gain quantitative information of the selected leakage model. Although very useful, the feedback information does not contain any information about the precision and accuracy of the selected leakage function. In Subsects. II-A and II-B we briefly summarize the basics of the stochastic approach (cf. [5], [8], [11] for details).

A. Notation and the Stochastic Model

In side-channel attacks the cryptographic key is guessed in small portions, referred to as subkeys k (here: single bytes). The letter $k \in \{0,1\}^s$ denotes a subkey, $x \in \{0,1\}^p$ a known part of the plaintext or the ciphertext. Random variables are represented with capital letters while their realizations[1] are denoted by the corresponding small letters. In particular, X assigns a random variable that assumes a small part (p bits) of the plaintexts or of the ciphertext. The term $E_Y(\cdot)$ denotes the expectation (or more colloquial, the average value) of a random variable Y. Vectors are written in bold face and estimates are assigned by the $\sim$ sign. The stochastic approach interprets the electrical current consumption[2] $i_t := i_t(x,k)$ at time t as a realization of a random variable $I_t(x,k)$ whose unknown distribution depends on the tuple (x,k). More precisely, as the left hand side of Fig. 1 a) depicts

$$I_t(x,k) = h_t(x,k) + R_t\,. \tag{1}$$

The leakage function $h_t(x,k)$ quantifies the deterministic part of the electrical current consumption and the random variable R_t quantifies the centered noise, which is independent of $h_t(x,k)$. W.l.o.g.[3] we may assume $E(R_t) = 0$, and further R_t is assumed to be normally distributed.

Note that $h_t(x,k)$ provides the most relevant information for constructive side-channel analysis. We note that if the stochastic approach shall be used as an attack tool in a second profiling step the joint density of $(R_{t_1}, \ldots, R_{t_m})$ is estimated for time instants $t_1 < \cdots < t_m$, and in the attack phase the attacker uses the information derived in the profiling steps to guess the unknown subkey, c.f., [5], [11].

B. Estimation of the Leakage Function $h_t(\cdot,\cdot)$

For each admissible subkey $k \in \{0,1\}^s$ we consider the restricted function $h_{t;k}\colon \{0,1\}^p \times \{k\} \to \mathbb{R}$ as an element of a 2^p-dimensional real subspace $\mathcal{F}_k := \{h'\colon \{0,1\}^p \times \{k\} \to \mathbb{R}\}$. Instead of estimating $h_{t;k}$ in $\mathcal{F}_k$ the stochastic approach aims at the best approximator $h^*_{t;k}$ in some appropriate subspace $\mathcal{F}_{u,t;k}$, which is spanned by u basis functions $g_{j,t;k}\colon \{0,1\}^p \times \{k\} \to \mathbb{R}$, $j = 0, \ldots, u-1$

$$\begin{aligned}\mathcal{F}_{u,t;k} := \quad & \{h'\colon \{0,1\}^p \times \{k\} \to \mathbb{R} \mid \\ & h' = \sum_{j=0}^{u-1} \beta'_j g_{j,t;k} \text{ with } \beta'_j \in \mathbb{R}\}.\end{aligned} \tag{2}$$

Note that the basis vectors $g_{0,t;k}(\cdot,k), \ldots, g_{u-1,t;k}(\cdot,k)$ should capture the relevant source of side-channel leakage with regard to the concrete implementation (cf. [5], [10], [11]). We denote the coefficients $\beta^*_{0,t;k}, \ldots, \beta^*_{u-1,t;k}$ of $h^*_{t;k}$ with regard to this basis as the *β-characteristic*. Let $i_t(x_1,k), \ldots, i_t(x_{N_1},k) \in \mathbb{R}$ denote N_1 measurements at time t, and let the real-valued $(N_1 \times u)$-matrix

$$A := \begin{pmatrix} g_{0,t;k}(x_1,k) & \ldots & g_{u-1,t;k}(x_1,k) \\ \vdots & \ddots & \vdots \\ g_{0,t;k}(x_{N_1},k) & \ldots & g_{u-1,t;k}(x_{N_1},k) \end{pmatrix}. \tag{3}$$

If the $(u \times u)$-matrix $A^T A$ is regular the normal equation $A^T A\mathbf{b} = \mathbf{A^T i_t}$ has a unique solution $\widetilde{\mathbf{b}}^*$, and accordingly

$$\widetilde{h}^*_{t;k}(\cdot,k) = \sum_{j=0}^{u-1} \widetilde{\beta}^*_{j,t;k} g_{j,t;k}(\cdot,k) \quad \text{with } \widetilde{\beta}^*_{j,t;k} := \widetilde{b}^*_j \tag{4}$$

is the least square estimate of $h^*_{t;k}$. Roughly speaking, the data-dependent current consumption $h_{t;k}$ is projected onto the subspace $\mathcal{F}_{u,t;k}$, and its image can be expressed by a linear combination of the basis functions $g_{j,t;k}(\cdot,k)$ weighted with the $\widetilde{\beta}^*_{j,t;k}$ coefficients, c.f., Fig. 1 b). As shown in [8] the β-characteristic reveals flaws of the implementation if the leakage model is chosen reasonably. Hence the β-characteristic provides quantitative information, which can be used for (re-)design methods. An overview of reasonable leakage models and their relevance for hardware implementations is given in the next section.

III. Selection of the Subspace

In this section we discuss properties of increasing subspaces. Figure 2 illustrates how leakage models with different subspaces capture transitions between registers of a combinational circuit part. The model with a 2-dimensional subspace[4] considers the joint electrical current consumption induced by all bit flips. The 9-dimensional subspace assumes that all bit lines leak independently. This model is appropriate if one only

[1] values assumed by these random variables

[2] the current consumption is proportional to the power consumption

[3] without loss of generality

[4] similar to the common Hamming Distance model, favored model for DPA

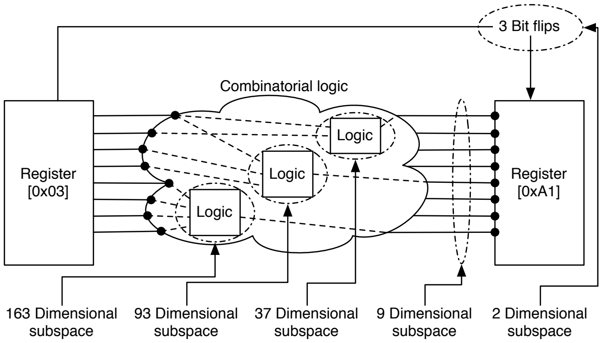

Fig. 2. Scheme of the effects captured by different subspaces

focuses on the bit flips inside the register. Leakage models with higher subspaces may be superior if additional switching activity of the combinatorial circuit occurs since they additionally capture data-dependent glitches. Fig. 2 illustrates the properties of several high-dimensional subspaces, which consider interactions between up to four bits. In the following we specify the leakage models with subspaces from dimension 2 to dimension 163. The target is the final round of an AES-128 cipher (key size of 128-bit) implementation in hardware.

The 2-dimensional subspace considers the Hamming Distance between the ciphertext and the intermediate register value of the 9th round. More precisely, $\mathcal{F}_{2,t;k}$ is spanned by the following basis vectors:

$$\begin{aligned} &g_{0,t;k}((x_{(z)},x_{(y)}),k_{(y)}) = 1 \\ &g_{1,t;k}((x_{(z)},x_{(y)}),k_{(y)}) = \\ &\qquad \mathrm{HW}\left(x_{(z)} \oplus S^{-1}(x_{(y)} \ \oplus \ k_{(y)})\right) - 4 \end{aligned} \tag{5}$$

where '(y)' and '(z)' label the respective key bytes (cf. [8] for details). Note that the constant function $g_{0,t;k}$ captures the expected level of the complete current consumption. Furthermore, for uniformly distributed pairs $(X_{(y)}, X_{(z)})$ we have $E_X(g_{1,t;k}((X_{(y)}, X_{(z)}), k_y)) = 0$ due to the subtraction of 4.

The 9-dimensional subspace aims at capturing the direct transitions bitwise, thus it is spanned by the basis vectors:

$$\begin{aligned} &g_{0,t;k}((x_{(z)},x_{(y)}),k_{(y)}) = 1 \\ &g_{j,t;k}((x_{(z)},x_{(y)}),k_{(y)}) = \\ &\quad 2\ ((x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_j - \tfrac{1}{2^1}) \quad \text{for } j = 1, \ldots, 8. \end{aligned} \tag{6}$$

As above $E_X(g_{j,t;k}((X_y, X_z), k_y)) = 0$ for $j = 1, \ldots, 8$ for uniformly chosen $(X_{(y)}, X_{(z)})$ due to the subtraction of $\frac{1}{2^1}$. Similarly, the expectation of the basis vectors in Eqs. (7) to (9) is 0, too.

If one assumes that the interaction between two bit lines may also cause leakage it is reasonable to add the following basis vectors

$$\begin{aligned} &g_{j,t;k}((x_{(z)},x_{(y)}),k_{(y)}) = \\ &2^2\ ((x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_1}(x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_2} \\ &-\frac{1}{2^2})) \text{ for } 9 \leq j \leq 37 \text{ and } 1 \leq j_1 < j_2 \leq 8. \end{aligned} \tag{7}$$

Moreover, the leakage arising from the transaction between three bit lines is captured by the following basis vectors:

$$\begin{aligned} &g_{j,t;k}(x_{(z)},x_{(y)}),k_{(y)}) = \\ &2^3\ ((x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_1}(x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_2} \\ &(x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_3} - \frac{1}{2^3})) \text{ for } 38 \leq j \leq 93 \\ &\qquad \text{and } 1 \leq j_1 < j_2 < j_3 \leq 8. \end{aligned} \tag{8}$$

The following basis vectors additionally capture the transaction between four bit lines:

$$\begin{aligned} &g_{j,t;k}((x_{(z)},x_{(y)}),k_{(y)}) = \\ &2^4\ ((x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_1}(x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_2} \\ &(x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_3}(x_{(z)} \oplus S^{-1}(x_{(y)} \oplus k_{(y)}))_{j_4} \\ &-\frac{1}{2^4})) \text{ for } 94 \leq j \leq 163 \text{ and } 1 \leq j_1 < j_2 < j_3 < j_4 \leq 8. \end{aligned} \tag{9}$$

Remark 1: (i) For a uniformly distributed random variable X in the general case $(h', h'') \mapsto E(h'(X,k) \cdot h''(X,k))$ defines an L^2 scalar product on $\mathcal{F}_k$. In our context clearly $X = (X_{(y)}, X_{(z)})$.

(ii) With regard to this scalar product all basis vectors from Eqs. (6) to (9) are normalized, which was the reason for introducing the factor 2^i. While the basis functions from Eq. (6) are even orthonormal, the others are not. An orthonormal basis can be determined with well-known algorithms.

However, the option of applying high-dimensional subspace based leakage models raises the question: How 'large' should the selected subspace $\mathcal{F}_{u,t;k}$ be? Of course, $\mathcal{F}_{u,t;k}$ might not contain the exact leakage function $h_{t;k}$ but the distance between the approximator $h^*_{t;k} \in \mathcal{F}_{u,t;k}$ and $h_{t;k}$ should be relatively small, c.f., Fig. 1b). We investigate this issue below.

IV. Suitability of the Selected Subspace

The efficiency of the stochastic approach depends significantly on the choice of the leakage model and thus of the subspace $\mathcal{F}_{u,t;k}$. A natural 'benchmark' is the attack efficiency, which allows a rating relative to other attacks. At least for design purposes, however, it would be more desirable to have absolute criteria for assessing the suitability of $\mathcal{F}_{u,t;k}$.

A. A Benchmark for Different Leakage Models

In [14] a new symmetry metric was discussed, which allows to verify the suitability of leakage models with regard to assumed symmetries of the leakage function. However, this definitely useful result covers only some aspects on whether the selected subspace is indeed appropriate. A related question is, how many basis vectors should be considered or, loosely speaking, how 'large' the subspace $\mathcal{F}_{u,t;k}$ should be. If $\mathcal{F}_{u,t;k}$ is selected too 'small' one clearly loses the information that is contained 'outside' $\mathcal{F}_{u,t;k}$. On the other hand, if $\dim(\mathcal{F}_{u,t;k})$ is unnecessarily large this may slow down the convergence rate of the least square estimate, which must be compensated by (maybe significantly) increasing the number of measurements. If the number of measurements is not sufficient, the estimate $\widetilde{h}^*_{t;k}$ might be worse than for a smaller subspace.

Definition 1: The L^2 distance between two functions $h', h'' \in \mathcal{F}_k$ is given by $\|h' - h''\| := \sqrt{2^{-p} \sum_{x \in \{0,1\}^p} (h'(x) - h''(x))^2}$.

Note that the L^2 distance corresponds to the scalar product introduced in Remark 1(i). The term $E_{X,R}(\cdot)$ stands for the expectation with regard to the random variables X and R. To simplify the notation we introduce the abbreviations $\Delta h_{t;k} := h_{t;k} - h^*_{t;k}$ and $\widetilde{\Delta} h_{t;k} := h_{t;k} - \widetilde{h}^*_{t;k}$. W.l.o.g. we may assume that $g_{0,t;k}, \ldots, g_{u-1,t;k}$ is an orthonormal basis of $\mathcal{F}_{u,t;k}$ (c.f., *Remark 1*), which is extended by suitable vectors $g_{u,t;k}, \ldots, g_{2^p-1,t;k}$ to an orthonormal basis of $\mathcal{F}_k$. For our purposes the L^2 distance $\|h_{t;k}(\cdot,k) - h^*_{t;k}(\cdot,k)\|$ provides all the information we are interested in, namely the approximation error $\Delta h_{t;k}(\cdot,k)$, resp. the estimated error $\widetilde{\Delta} h_{t;k}(\cdot,k)$. Unfortunately, this value cannot directly be computed since the exact leakage function $h_{t;k}(\cdot,k)$ is unknown. Let X denote a uniformly distributed random variables that assumes values in $\{0,1\}^p$, then

$$\|\Delta h_{t;k}(\cdot,k)\|^2 = E_X\left((h_{t;k}(X,k) - h^*_{t;k}(X,k))^2\right). \quad (10)$$

Equation (11) provides an equation for the unknown L^2 distance, and Ineq. (12) provides an upper bound.

$$\begin{aligned} & E_{X,R}\left((I_t(X,k) - h^*_{t;k}(X,k))^2\right) \\ = \; & E_{X,R}\left((\Delta h_{t;k}(X,k) + R_t)^2\right) \\ = \; & E_X\left(\Delta h_{t;k}(X,k)^2\right) + E_R(R_t^2) \quad (11) \\ \geq \; & E_X(\Delta h_{t;k}(X,k)^2) = \|\Delta h_{t;k}(\cdot,k)\|^2 = \sum_{j=u}^{2^p-1} \beta^2_{j,t;k}. \quad (12) \end{aligned}$$

The left-hand term of (11) can easily be estimated: From N traces one computes the term

$$\frac{1}{N} \sum_{j=1}^{N} \left(i_t(x_j,k) - \widetilde{h}^*_{t;k}(x_j,k)\right)^2 \quad (13)$$

where the values $x_1, \ldots, x_N$ should be drawn from a uniform distribution. The smaller the noise the more meaningful Ineq. (12) is.

Nevertheless, we also provide an estimator for $E(R_t^2)$. Recall that for each pair $(x,k) \in \{0,1\}^p \times \{0,1\}^s$ the term $I_t(x,k)$ denotes a random variable with unknown distribution that depends on (x,k). Now let $I'_t(x,k)$ be an independent random variable, which has the same distribution as $I_t(x,k)$. This means

$$\begin{aligned} I_t(x,k) = h_{t;k}(x,k) + R_t \text{ and } I'_t(x,k) = h_{t;k}(x,k) + R'_t \\ \text{with } E_R(R_t) = E_{R'}(R'_t) = 0 \quad (14) \end{aligned}$$

with independent and identically distributed random variables R_t and R'_t. This implies

$$\begin{aligned} E_X\left((I_t(X,k) - I'_t(X,k))^2\right) &= E_{R,R'}\left((R_t - R'_t)^2\right) \\ &= 2E_R(R_t^2). \quad (15) \end{aligned}$$

From (16) we deduce an estimator for $E_R(R_t^2)$

$$\widetilde{E_R(R_t^2)} = \frac{1}{2N_2} \sum_{v=1}^{N_2} \left(i_t(x_{2v-1},k) - i_t(x_{2v},k)\right)^2 \quad (16)$$

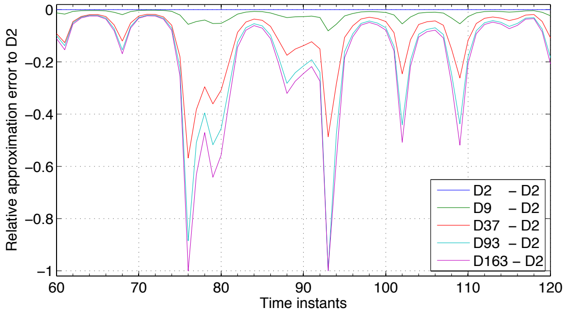

Fig. 3. Relative approximation errors to the model with a 2-dim subspace

Here $i_t(x_1,k), \ldots, i_t(x_{2N_2},k)$ denotes a set of randomly selected $2N_2$ traces with $x_{2v-1} = x_{2v}$ for $1 \leq v \leq N_2$. Applying Eq. (13) and Eq. (16) one finally obtains an estimate for $\|\widetilde{\Delta} h_{t;k}(\cdot,k)\|^2$.

Remark 2: If symmetries exist (as in Eq. (6) to (9)) the distance $\|\Delta h_{t;k}(\cdot,k)\|$ identical for all subkeys $k \in \{0,1\}^s$ (c.f., [14], Subsect. III.B).

B. Practical Estimation of the Approximation Error

We applied our theoretical approach to measurements performed on the SASEBO-GII FPGA board. We focus on the final encryption round of a parallel implemented AES-128 design, which uses ten clock cycles for one plaintext encryption. We decided to use a composite-field based SBox design [15] in order to assure a certain logic depth and thereby exploitable data-dependent glitches.

In the following we abbreviate $\|\widetilde{\Delta} h_{t;k}(\cdot,k)\|$ by $\widetilde{\Delta}^{(u)}_{t;k}$ when $h^*_{t;k}(\cdot,k)$ is an element of a u-dimensional subspace. For example, $\widetilde{\Delta}^{(2)}_{t;k}$ refers to $\|\widetilde{\Delta} h_{t;k}(\cdot,k)\|$ with $h^*_{t;k}(\cdot,k) \in \mathcal{F}_{2,t;k}$. For each of the five leakage models and thus for each of the five different subspaces, we estimated $\widetilde{h}^*_{t;k}(\cdot,k)$ from 500.000 traces. Note that the estimation of $E_R(R_t^2)$ (c.f. Eq. (16)) is independent of the leakage function. A set of 500.000 traces were used to determine $\|\Delta h_{t,k}(\cdot,k)\|^2$ (cf. Eq. (10)) by calculating the differences between the measured current and the estimation $\widetilde{h}^*_{t;k}(\cdot,k)$ (c.f. Eq. (13)).

The experiments demonstrate that the differences in $\widetilde{\Delta}^{(u)}_{t;k}$ for $u \in \{2, 9, 37, 93, 163\}$ are relatively small compared to the absolute value of $\widetilde{\Delta}^{(u)}_{t;k}$. Moreover, the absolute values depend on the concrete implementation. To illustrate our results we compared $\widetilde{\Delta}^{(u)}_{t;k}$ with $\widetilde{\Delta}^{(2)}_{t;k}$, which serves as a reference value. We computed $(\widetilde{\Delta}^{(u)}_{t;k} - \widetilde{\Delta}^{(2)}_{t;k})/\widetilde{\Delta}^{(2)}_{t;k}$ for $u \in \{2, 9, 37, 93, 163\}$ at each time instant. Figure 3 plots this error coefficient for the 11^{th} byte of the final round key. The different subspaces denoted by capital 'D', followed by their dimensions. In particular, *D2 - D9* refers to $(\widetilde{\Delta}^{(9)}_{t;k} - \widetilde{\Delta}^{(2)}_{t;k})/\widetilde{\Delta}^{(2)}_{t;k}$.

Figure 3 shows that the approximation error of $\widetilde{h}^*_{t;k} \in \mathcal{F}_{u,t;k}$ becomes significantly smaller as u increases. Due to different switching activities in the circuit this trend is (quantitatively) not identical over all time instants. Moreover, $\widetilde{\Delta}^{(u)}_{t;k}$ results from the difference of large values of similar size so that precise estimates of the ratio require large samples. If $\|\widetilde{\Delta}h_{t;k}(\cdot,k)\|^2 < 0$ (rare event, estimation error) we set $\widetilde{\Delta}^{(u)}_{t;k} := 0$. A second interesting observation is that for $u \in \{37, 93, 163\}$ the minimum value of $(\widetilde{\Delta}^{(u)}_{t;k} - \widetilde{\Delta}^{(2)}_{t;k})/\widetilde{\Delta}^{(2)}_{t;k}$ occurs at the same time instant while $(\widetilde{\Delta}^{(9)}_{t;k} - \widetilde{\Delta}^{(2)}_{t;k})/\widetilde{\Delta}^{(2)}_{t;k}$ attains its minimum some time instants later than the high-dimensional subspaces, confirming the assumption from Sect. III. Accordingly, the experiments verify that leakage models with high-dimensional subspaces do not only consider bit flips within the register but additionally capture data-dependent glitches.

V. SNR as Benchmark

In Sect. IV we developed a method to estimate $\|\widetilde{\Delta}h_{t;k}(\cdot,k)\|$, which quantifies the approximation error for the selected subspace $\mathcal{F}_{u,t;k}$. This metric discloses inaccuracies of the selected subspace, which in turn affects the success rate of an attack. However, this metric neither includes the algorithmic noise of parallel active circuits nor the noise inherited from the measurement process. A common way to characterize the quality of a measured trace is the signal-to-noise ratio (SNR). It has a great influence on the success rate of a side-channel attack, c.f. [16], [17], and thus is also an important characteristic of any security implementation. For instance, the SNR may be used to quantify the strength of countermeasures. In this section we use the stochastic approach to estimate the SNR. In particular, this method has the advantage that it is not constrained to some fixed leakage model (like the Hamming Distance).

A. SNR Leakage Estimation

Generally, the SNR is defined as $\frac{\mathrm{Var}(signal)}{\mathrm{Var}(noise)}$, the ratio between the variance of the determinable signal and the noise of the measurement. In the context of side-channel analysis a more precise definition is given in [17] by

$$\mathrm{SNR} = \frac{\mathrm{Var}(P_{data})}{\mathrm{Var}(P_{others} + P_{noise})}\,. \tag{17}$$

As mentioned above we focus on the electrical current consumption, which is proportional to the power consumption and all their additive components, c.f., Eq. (18).

$$\frac{\mathrm{Var}(P_{data})}{\mathrm{Var}(P_{others} + P_{noise})} \sim \frac{\mathrm{Var}(I_{data})}{\mathrm{Var}(I_{others} + I_{noise})}\,. \tag{18}$$

I_{data} denotes the exploitable power consumption. Thus, it is defined by the current consumption of the data-dependent deterministic part $h^*_{t;k}$. Further, I_{noise} denotes the power consumption due to noise, which is captured by R_t. Moreover, I_{others} denotes the current consumption of parallel running activities of the circuit and, of course, the approximation error addressed in Sect. IV. We maintain the abbreviations and conventions from the previous sections. In particular, we assume that $g_{0,t;k}(\cdot,k), \ldots, g_{u-1,t;k}(\cdot,k)$ is an orthonormal basis. Straight-forward computations yield

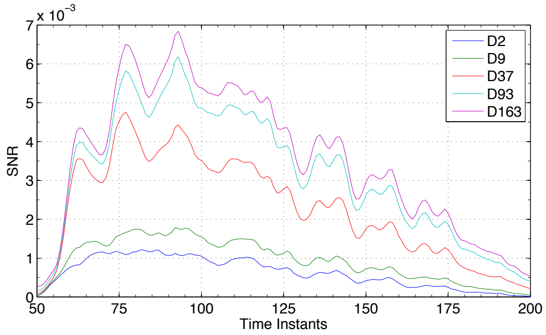

Fig. 4. SNR Evaluation over all five subspaces

$$\begin{aligned}\mathrm{Var}(I_{data}) &= \mathrm{Var}_X(h^*_{t;k}(X,k)) \\ &= E_X(h^*_{t;k}(X,k)^2) - E^2_X(h^*_{t;k}(X,k)) \\ &= \sum_{j=0}^{u-1}\beta^2_{j,t;k} - \beta^2_{0,t;k} = \sum_{j=1}^{u-1}\beta^2_{j,t;k}\,. \end{aligned} \tag{19}$$

Similarly,

$$\begin{aligned} &\mathrm{Var}(I_{others} + I_{noise}) = \mathrm{Var}_{X,R}(\Delta h_{t;k}(X,k) + R_t) \\ = \quad &\mathrm{Var}_{X,R}(I_t(X,k) - h^*_{t;k}(X,k))\,. \end{aligned} \tag{20}$$

Combining (19) with (20) yields an estimator for the signal-to-noise ratio ($\widetilde{\mathrm{SNR}}$)

$$\frac{\sum_{j=1}^{u-1}\widetilde{\beta}^2_{j,t;k}}{\mathrm{empVar}\left(i_t(x_1,k)-\widetilde{h}^*_{t,k}(x_1,k),\ldots,i_t(x_N,k)-\widetilde{h}^*_{t,k}(x_N,k)\right)} \tag{21}$$

As usual, $i_t(x_1,k),\ldots,i_t(x_N,k)$ denotes a set of N electrical current measurements and $\mathrm{empVar}(\cdot)$ denotes the empirical variance. Compared to the error approximation in Sect. IV the SNR gives no information on the accuracy of the selected subspace-based leakage model. For side-channel analysis the SNR quantifies the relation between exploitable information and the 'sum' of the power consumption of other (data-dependent) activities that run in parallel (here: other S-boxes) and noise. The SNR quantifies how much useful side-channel information a leakage function extracts from the traces relative to the existing noise.

B. Experimental SNR Estimation

We calculate $\widetilde{SNR}$ for the five different subspaces, which were introduced in Sect. III. To compare the approximation error from Sect. IV with the SNR we focused on the same round key byte and used the same power traces. Figure 4 depicts the $\widetilde{SNR}$ for the five different subspaces over the selected time instants of the final encryption round. The leakage models are denoted as in the previous analysis, c.f., Subsect. IV-B. One can clearly see that the $\widetilde{SNR}$ is maximal for the 163-dimensional subspace. Accordingly, this leakage model extracts the most leakage information from the measured set of electrical current traces. Obviously the precision of the subspace of the leakage model, c.f., Sect. IV, affects the SNR. Improvements in the precision of the leakage model

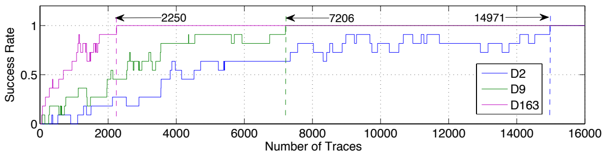

Fig. 5. Success rate of three different subspaces

increase the $\widetilde{SNR}$, which enhances the distinguishability between the side-channel leakage and the noise. Thus the $\widetilde{SNR}$ refers directly to the efficiency of the leakage function for an attack, c.f. [16], [17]. Due the data-dependent glitches for the analyzed AES-128 implementation leakage models exploiting high-dimensional subspaces show much better results than one with low-dimensional subspaces.

Success rate: To verify that the discussed methods may indeed serve as reliable indicators for the degree of vulnerability of a cryptographic design by side-channel attacks we performed ten side-channel attacks on different sets of power traces. We applied the commonly used success rate [9] to evaluate the side-channel resistance. In order to keep the information illustrative Fig. 5 only considers the 2-, 9-, and 163-dimensional subspaces based leakage models. Table I provides the minimum number of traces needed for a successful attack for all discussed leakage models. The results show that low-dimensional leakage models are clearly less efficient than the 163-dimensional version, confirming the results that were derived from the methods introduced in Sect. V and Sect. IV.

VI. Conclusion

We investigated the precision of leakage functions, in particular of leakage models corresponding to high-dimensional subspaces. We introduced two metrics, the L^2 distance $\|\Delta h_{t;k}\|$ and the SNR, which can be used to quantify the accuracy of selected subspace $\mathcal{F}_{u,t;k}$, and thus may serve as useful tools for secure design. For an AES-128 block cipher hardware implementation we exemplarily discussed several leakage models with high-dimensional subspaces. We investigated the accuracy and precision of these leakage functions with our proposed methods, and we compared these results with the success rate of conducted side-channel attacks. In our experiments these two metrics led to the same efficiency ranking of the leakage functions as concrete attacks on the implementation. We mention that even for high-dimensional subspaces the computation time for our metrics is not the limiting factor; the acquisition time still dominates the duration of the side-channel evaluation. In particular, leakage models with high-dimensional subspace reduced the required number of traces up to a sixth compared to the Hamming Distance model.

TABLE I
Success rate for all leakage models

Subspace [dim]	2	9	37	93	163
# Traces for success rate=1	14971	7206	3137	2881	2250

Acknowledgment

The work presented in this contribution was supported by the German Federal Ministry of Education and Research (BMBF) in the project *Resist* through grant number 01IS10027A and CASED (www.cased.de).

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO*, ser. Lecture Notes in Computer Science, M. J. Wiener, Ed., vol. 1666. Springer, 1999, pp. 388–397.

[2] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *CHES*, ser. Lecture Notes in Computer Science, M. Joye and J.-J. Quisquater, Eds., vol. 3156. Springer, 2004, pp. 16–29.

[3] B. Gierlichs, L. Batina, B. Preneel, and I. Verbauwhede, "Revisiting Higher-Order DPA Attacks: Multivariate Mutual Information Analysis," in *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference*, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5985. San Francisco,CA,USA: Springer-Verlag, 2010, pp. 221–234.

[4] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *CHES*, ser. Lecture Notes in Computer Science, B. Kaliski, Çetin Kaya Koç, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 13–28.

[5] W. Schindler, K. Lemke, and C. Paar, "A stochastic model for differential side channel cryptanalysis," in *CHES*, ser. Lecture Notes in Computer Science, J. R. Rao and B. Sunar, Eds., vol. 3659. Springer, 2005, pp. 30–46.

[6] J. Doget, E. Prouff, M. Rivain, and F.-X. Standaert, "Univariate Side Channel Attacks and Leakage Modeling," *Journal of Cryptographic Engineering*, vol. 1, pp. 123–144, 2011.

[7] M. A. Elaabid and S. Guilley, "Practical improvements of profiled side-channel attacks on a hardware crypto-accelerator," in *AFRICACRYPT*, ser. Lecture Notes in Computer Science, D. J. Bernstein and T. Lange, Eds., vol. 6055. Springer, 2010, pp. 243–260.

[8] M. Kasper, W. Schindler, and M. Stöttinger, "A Stochastic Method for Security Evaluation of Cryptographic FPGA Implementations," in *FPT 2010*. IEEE Press, 2010, pp. 146–154.

[9] B. Gierlichs, K. Lemke-Rust, and C. Paar, "Templates vs. stochastic methods," in *CHES*, ser. Lecture Notes in Computer Science, L. Goubin and M. Matsui, Eds., vol. 4249. Springer, 2006, pp. 15–29.

[10] K. Lemke-Rust and C. Paar, "Analyzing side channel leakage of masked implementations with stochastic methods," in *ESORICS*, ser. Lecture Notes in Computer Science, J. Biskup and J. Lopez, Eds., vol. 4734. Springer, 2007, pp. 454–468.

[11] W. Schindler, "Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking," *Math. Crypt.*, vol. 2, pp. 291–310, 2008.

[12] F.-X. Standaert, F. Koeune, and W. Schindler, "How to compare profiled side-channel attacks?" in *ACNS*, ser. Lecture Notes in Computer Science, M. Abdalla, D. Pointcheval, P.-A. Fouque, and D. Vergnaud, Eds., vol. 5536, 2009, pp. 485–498.

[13] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.

[14] A. Heuser, M. Kasper, W. Schindler, and M. Stoettinger, "How a Symmetry Metric Assists Side-Channel Evaluation - A Novel Model Verification Method for Power Analysis," in *14th EUROMICRO Conference on Digital System Design (DSD2011)*, P. Kitsos, Ed. IEEE Press, Sep. 2011, pp. 674 – 682.

[15] S. Morioka and A. Satoh, "An optimized s-box circuit architecture for low power aes design," in *CHES*, ser. Lecture Notes in Computer Science, B. S. K. Jr., Çetin Kaya Koç, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 172–186.

[16] S. Guilley, H. Maghrebi, Y. Souissi, L. Sauvage, and J. Danger, "Quantifying the Quality of Side-Channel Acquisition," in *COSADE*, 2011, pp. 16–28.

[17] S. Mangard, T. Popp, and M. E. Oswald, *Power Analysis Attacks - Revealing the Secrets of Smart Cards*. Springer, 2007.